

CLAIMS

We claim:

1. A method for providing local gateway support for multiple overlapping remote networks, comprising the steps of:
 - loading a plurality of overlapping connections, each including an inbound packet having a source IP address;
 - for each said connection, binding said source IP address in a bind table with an internally routable and system-wide unique source IP address from an internal address pool; and
 - network address translating outbound packets, each said outbound packet having a destination IP address, to determine a virtual private network connection for receiving said outbound packet.

1 2. The method of claim 1, further comprising the steps of:

2 filtering said outbound packet to determine a first
3 connection name;

4 determining from said bind table a second connection
5 name;

6 responsive to said first and second connection names
7 comparing equal, processing said outbound packet into a
8 VPN tunnel using a security association database
9 determined by said first connection name; and

10 responsive to said first and second connection names
11 comparing not equal, processing said outbound packet
12 into a VPN tunnel using a security association database
13 determined by said second connection name.

1 3. A local gateway system, comprising:

2 an address pool for storing a plurality of internally
3 routable and system wide, nonconflicting network
4 addresses;

5 an address bind table for binding a conflicting source
6 address from an inbound packet from a remote network to
7 a connection name and to a unique network address from
8 said address pool;

9 a filter rules table responsive to an outbound packet
10 for determining a first connection indicia;

11 said address bind table further responsive to said
12 outbound packet for determining a second connection
13 indicia; and

14 said local gateway system being responsive to said
15 first and second connection indicia comparing equal for
16 processing said outbound packet to a communications
17 tunnel using a first security association determined by
18 said first connection indicia, and responsive to said
19 first and second connection indicia comparing not equal
20 for processing said outbound packet to a communications
21 tunnel using a second security association determined
22 by said second connection indicia.

1 4. A program storage device readable by a machine,
2 tangibly embodying a program of instructions executable by a
3 machine to perform method steps for providing local gateway
4 support for multiple overlapping remote networks, said
5 method steps comprising:

6 loading a plurality of overlapping connections, each
7 including an inbound packet having a source IP address;

8 for each said connection, binding said source IP
9 address in a bind table with an internally routable and
10 system-wide unique source IP address from an internal
11 address pool; and

12 network address translating outbound packets, each said
13 outbound packet having a destination IP address, to
14 determine a virtual private network connection for
15 receiving said outbound packet.

1 5. The program storage device of claim 4, said method
2 steps further comprising:

3 filtering said outbound packet to determine a first
4 connection name;

5 determining from said bind table a second connection
6 name;

7 responsive to said first and second connection names
8 comparing equal, processing said outbound packet into a
9 VPN tunnel using a security association database
10 determined by said first connection name; and

11 responsive to said first and second connection names
12 comparing not equal, processing said outbound packet
13 into a VPN tunnel using a security association database
14 determined by said second connection name.

1 6. A computer program product or computer program element
2 for providing local gateway support for multiple overlapping
3 remote networks, according to method steps comprising:

4 loading a plurality of overlapping connections, each
5 including an inbound packet having a source IP address;

6 for each said connection, binding said source IP
7 address in a bind table with an internally routable and
8 system-wide unique source IP address from an internal
9 address pool; and

10 network address translating outbound packets, each said
11 outbound packet having a destination IP address, to
12 determine a virtual private network connection for
13 receiving said outbound packet.

1 7. A local gateway system for processing inbound and
2 outbound packets with respect to a local network and a
3 plurality of remote nodes having potentially overlapping
4 addresses, comprising:

5 an address pool component;

6 an address bind table component;

7 a filter rules table component;

8 a security association component;

9 an entry in said address bind table component including
10 a left hand side (LHS) address field, a right hand side
11 (RHS) address field, and first connection name field;

12 an entry in said filter rules table component including
13 source IP address (sip), destination IP address (dip),
14 source port, destination port, second connection name,
15 and action field;

16 said address pool component including a pool of sip
17 addresses administratively reserved and uniquely
18 routable within said local network;

19 a security association in said security association
20 component including third connection name and security
21 association data;

22 first logic responsive to an inbound packet for
23 dynamically binding in said address bind table
24 component the inbound packet sip with a local sip
25 selected from said address pool component and first
26 connection indicia;

27 second logic responsive to an outbound packet for
28 accessing said filter rules table component to
29 determine filter derived connection indicia;

30 third logic responsive to said outbound packet for
31 accessing said address bind table component to
32 determine corresponding bind table derived connection
33 indicia; and

34 fourth logic responsive to said filter derived
35 connection indicia and said bind table derived
36 connection indicia comparing equal for accessing said
37 security association component to select security
38 association data corresponding to said filter derived
39 connection data for processing said outbound packet,
40 and responsive to said filter derived connection
41 indicia and said bind table derived connection indicia
42 comparing not equal for accessing said security
43 association component to select security association
44 data corresponding to said bind table derived
45 connection indicia for processing said outbound packet.

1 8. The local gateway system of claim 7, further
2 comprising:

3 said action field selectively containing deny, permit,
4 and IP Sec required indicia; and

5 said second logic being responsive to said outbound
6 packet corresponding to a filter having an action field
7 containing said IP Sec required indicia for initiating
8 execution of said third logic.

1 9. A method for operating a local gateway, comprising the
2 steps of:

3 receiving an inbound packet on a network connection
4 from a remote node; and

5 applying source-in network address translation to
6 establish dynamic binding of the source IP address of
7 said inbound packet with an internally routable and
8 system wide unique source-in IP address and a
9 connection name.

1 10. The method of claim 9, further comprising the steps of:

2 receiving an outbound packet from an internal node;

3 filtering said outbound packet to determine a first
4 connection;

5 selectively determining a second connection from a
6 connection name bound to said unique source-in IP
7 address corresponding to the destination-out IP address
8 of said outbound packet; and

9 selectively overriding said first connection by said
10 second connection.

1 11. The method of claim 10, further comprising the step of:

2 tunneling said outbound packet to said remote node
3 responsive to security association data selectively
4 corresponding to said first connection or said second
5 connection.

1 12. The method of claim 11, further comprising the step of:
2 overriding said first connection by said second
3 connection responsive to said first connection and said
4 second connection comparing not equal.

1 13. A program storage device readable by a machine,
2 tangibly embodying a program of instructions executable by a
3 machine to perform method steps for providing local gateway
4 support for multiple overlapping remote networks, said
5 method steps comprising:

6 receiving an inbound packet on a network connection
7 from a remote node; and

8 applying source-in network address translation to
9 establish dynamic binding of the source IP address of
10 said inbound packet with an internally routable and
11 system wide unique source-in IP address and a
12 connection name.

1 14. The program storage device of claim 13, said method
2 steps further comprising:

3 receiving an outbound packet from an internal node;

4 filtering said outbound packet to determine a first
5 connection;

6 selectively determining a second connection from a
7 connection name bound to said unique source-in IP
8 address corresponding to the destination-out IP address
9 of said outbound packet; and

10 selectively overriding said first connection by said
11 second connection.

1 15. The program storage device of claim 14, said method
2 steps further comprising:

3 tunneling said outbound packet to said remote node
4 responsive to security association data selectively
5 corresponding to said first connection or said second
6 connection.

1 16. The program storage device of claim 15, said method
2 steps further comprising:

3 overriding said first connection by said second
4 connection responsive to said first connection and said
5 second connection comparing not equal.

1 17. A communication method, comprising the steps of:

2 operating a remote gateway to initiate a connection
3 with a local gateway;

4 sending from a remote node at said remote gateway an
5 inbound packet addressed by a destination address to a
6 local node at said local gateway and a remote node
7 source address identifying said remote node;

8 operating said local gateway to decapsulate said
9 inbound packet;

10 operating said local gateway to determine that said
11 inbound packet requires source-in network address
12 translation and that no existing address bind exists
13 for said inbound packet;

14 operating said local gateway to choose a pool address
15 and create a binding table entry binding said remote
16 node source address to said pool address and a unique
17 connection name;

18 replacing said remote node source address with said
19 pool address and forwarding said inbound packet to said
20 local node;

21 receiving at said local gateway an outbound packet
22 having as its destination address said pool address;

23 filtering said outbound packet to identify
24 corresponding connection indicia;

25 finding in said binding table an entry corresponding to
26 said outbound packet, converting said destination
27 address to said remote node source address, and
28 returning said unique connection name;

29 responsive to said unique connection name, selecting
30 security association data; and

31 responsive to said security association data, tunneling
32 said outbound packet to said remote node.

1 18. The method of claim 17, said remote node being one of a
2 plurality of remote nodes having overlapping addresses.

1 19. The method of claim 18, further comprising the steps
2 of:

3 comparing said corresponding connection indicia and
4 said unique connection name; and

5 responsive to said corresponding connection indicia and
6 said unique connection name comparing equal, selecting
7 security association data corresponding to said
8 corresponding connection indicia.

1 20. A method for operating a local gateway for controlling
2 communication between a local node and a remote node,
3 comprising the steps of:

4 receiving an inbound packet on a network connection
5 from a remote node, said inbound packet characterized
6 by a first source address identifying said remote node
7 and a first destination address identifying said local
8 node; and

9 applying source-in network address translation to
10 establish dynamic binding of said first source address
11 with an internally routable and system wide unique
12 second source address and a first connection name.

1 21. The method of claim 20, further comprising the steps
2 of:

3 establishing said dynamic binding by creating a binding
4 entry in an address bind table with a bind entry left
5 hand side set equal to said second source address

6 selected from a local address pool, a bind entry right
7 hand side set equal to said first source address, and
8 said first connection name.

1 22. The method of claim 21, further comprising the steps
2 of:

3 receiving from said local node an outgoing packet
4 intended for said remote node and having identifying
5 indicia including a second destination address;

6 filtering said outgoing packet to find a filter rule
7 having a second connection name associated with said
8 identifying indicia;

9 responsive to said second connection name, identifying
10 a filter derived security association;

11 responsive to said filter rule requiring source-in
12 network address translation, searching said address
13 bind table for a matching binding entry having a bind
14 entry left hand side corresponding to said second
15 destination address, and setting said second

16 destination address equal to said bind entry right hand
17 side;

18 responsive to said first connection name selected from
19 said matching binding entry, identifying a binding
20 table derived security association; and

21 selectively responsive to said filter derived security
22 association or said binding table derived security
23 association, processing said outbound packet into a
24 tunnel for communication to said remote node.

1 23. The method of claim 22, further comprising the steps
2 of:

3 responsive to said first connection name selected from
4 said matching binding entry and said second connection
5 name comparing not equal, selecting said binding table
6 derived security association for processing said
7 outbound packet.

1 24. A program storage device readable by a machine,
2 tangibly embodying a program of instructions executable by a
3 machine to perform method steps for providing local gateway
4 support for multiple overlapping remote networks, said
5 method steps comprising:

6 operating a remote gateway to initiate a connection
7 with a local gateway;

8 sending from a remote node at said remote gateway an
9 inbound packet addressed by a destination address to
10 said local node at said local gateway and a remote node
11 source address identifying said remote node;

12 operating said local gateway to decapsulate said
13 inbound packet;

14 operating said local gateway to determine that said
15 inbound packet requires source-in network address
16 translation and that no existing address bind exists
17 for said inbound packet;

18 operating said local gateway to choose a pool address
19 and create a binding table entry binding said remote

20 node source address to said pool address and a unique
21 connection name;

22 replacing said remote node source address with said
23 pool address and forwarding said inbound packet to said
24 local node;

25 receiving at said local gateway an outbound packet
26 having as its destination address said pool address;

27 filtering said outbound packet to identify
28 corresponding connection indicia;

29 finding in said binding table an entry corresponding to
30 said outbound packet, converting said destination
31 address to said remote node source address, and
32 returning said unique connection name;

33 responsive to said unique connection name, selecting
34 security association data; and

35 responsive to said security association data, tunneling
36 said outbound packet to said remote node.

1 25. A program storage device readable by a machine,
2 tangibly embodying a program of instructions executable by a
3 machine to perform method steps for providing local gateway
4 support for multiple overlapping remote networks, said
5 method steps comprising:

6 receiving an inbound packet on a network connection
7 from a remote node, said inbound packet characterized
8 by a first source address identifying said remote node
9 and a first destination address identifying said local
10 node; and

11 applying source-in network address translation to
12 establish dynamic binding of said first source address
13 with an internally routable and system wide unique
14 second source address and a first connection name.

1 26. The program storage device of claim 25, said method
2 steps further comprising:

3 establishing said dynamic binding by creating a binding
4 entry in an address bind table with a bind entry left

5 hand side set equal to said second source address
6 selected from a local address pool, a bind entry right
7 hand side set equal to said first source address, and
8 said first connection name.

1 27. The program storage device of claim 26, said method
2 steps further comprising:

3 receiving from said local node an outgoing packet
4 intended for said remote node and having identifying
5 indicia including a second destination address;

6 filtering said outgoing packet to find a filter rule
7 having a second connection name associated with said
8 identifying indicia;

9 responsive to said second connection name, identifying
10 a filter derived security association;

11 responsive to said filter rule requiring source-in
12 network address translation, searching said address
13 bind table for a matching binding entry having a bind
14 entry left hand side corresponding to said second

15 destination address, and setting said second
16 destination address equal to said bind entry right hand
17 side;

18 responsive to said first connection name selected from
19 said matching binding entry, identifying a binding
20 table derived security association; and

21 selectively responsive to said filter derived security
22 association or said binding table derived security
23 association, processing said outbound packet into a
24 tunnel for communication to said remote node.

1 28. The program storage device of claim 27, said method
2 steps further comprising:

3 responsive to said first connection name selected from
4 said matching binding entry and said second connection
5 name comparing not equal, selecting said binding table
6 derived security association for processing said
7 outbound packet.